DES, AES AND TRIPLE DES: SYMMETRIC KEY CRYPTOGRAPHY ALGORITHM

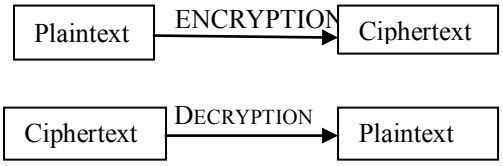
RIMPI DEBNATH, PRIYANKA AGRAWAL, GEETANJALI VAISHNAV

Abstract— **Security is one of the most challenging aspects in the internet and networks. Cryptography is the one of the main categories that converts information into an unreadable form. Cryptography allows people to carry their confidential data over the network without worries and insecurity. This paper provide comparison between three symmetric key cryptosystem i.e. DES, AES and triple DES.**

***Index Terms*—cryptography, DES, AES, triple DES, symmetric key.**

I.INTRODUCTION

Cryptography is referred as "the study of secret". Encryption process is basically used for converting normal text into unreadable form. Whereas decryption process is just the reverse process of encryption in which the encrypted text is converted back to its normal form.



Steps involved in the conventional encryption:

- A sender wants to send a message to the recipient.
- The original message is known as Plaintext.
- The original message which is to be send by the sender is encrypted.
- The encrypted message is known as cipher text.
- Ciphertext is different from the original message.
- Ciphertext is the unreadable form of plaintext.
- The ciphertext is then decrypted by the recipient.
- Recipient then gets the original message by decrypting the ciphertext using same algorithm and key.

The objectives of the cryptography regarding the security are:

Confidentiality, authentication, integrity and non-repudiation.

Confidentiality ensures the secret of the information. If any unauthorized users try to access the data remains encrypted and is unreadable to the intruders.

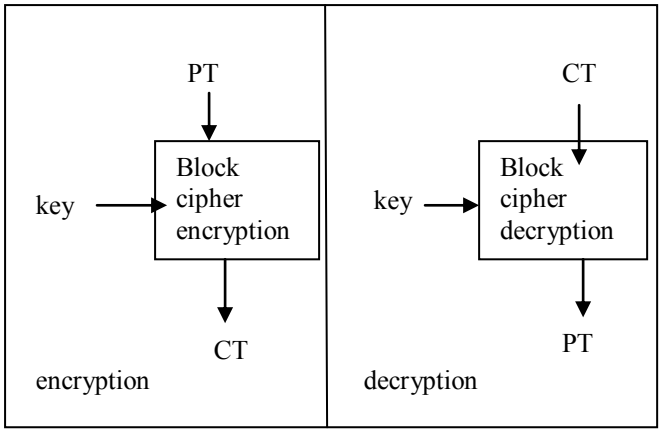
Authentication is concerned with entities identification. It ensures that the receiver and the transmitters are the right entities.

Integrity makes sure that message is not altered or corrupted.

Non-repudiation is a part of the system which keeps record of previously occurred events. Due to this property a receiver cannot declare that the message was not received.

DCLIII.BLOCK CIPHER

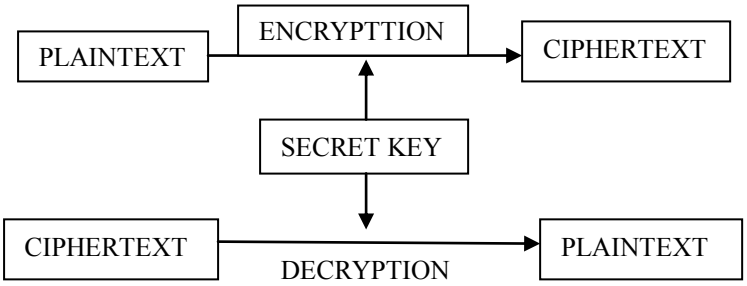
In Cryptography, a block cipher is a symmetric key cipher, which operates on fixed-length groups of bits, termed as blocks. A block cipher takes input of 128 bit of plaintext and output 128 bits of ciphertext.



In block cipher of the block size of the data is more than 128 bits then the encryption is done using stream cipher. As in block cipher the encryption is done of each block whereas in stream cipher encryption is done of single character.

DCLIIDCLIIDCLII.SYMMETRIC KEY CRYPTOGRAPHY

It is also known as single key cryptography. As it uses a single key. In this encryption process the receiver and the sender uses a single secret key or shared key. Given a message called plaintext and the key, encryption produces unreadable data, which is of the same length as the plaintext. Decryption is the reverse of encryption, and it uses the same key as encryption.



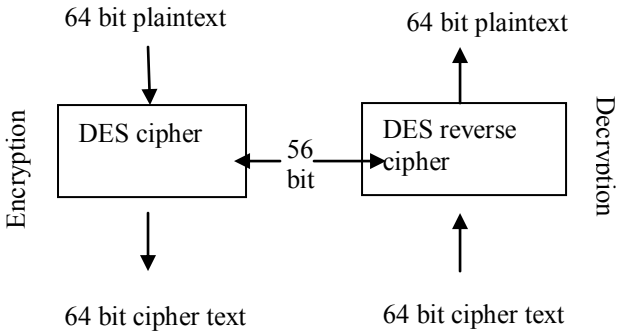
).

ISSN: 2278 – 7798

IV.BACKGROUND STUDY

A) Compared Algorithms:

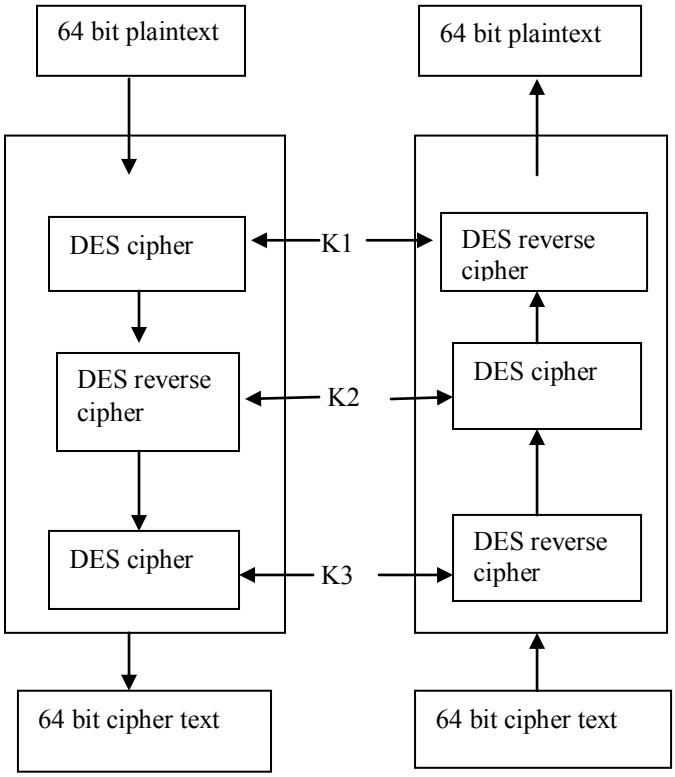
DES: (Data Encryption Standard), was the first encryption standard to be published by NIST (National Institute of Standards and Technology). DES is a Festal-type Substitution-Permutation Network (SPN) cipher. It was designed by IBM based on their Lucifer cipher. DES became a standard in 1974 (www.tropsoft.com). It uses 64 bit key. but practically it is more efficient to use 56 bit key. It uses both permutation and substitution. There are number of attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher.



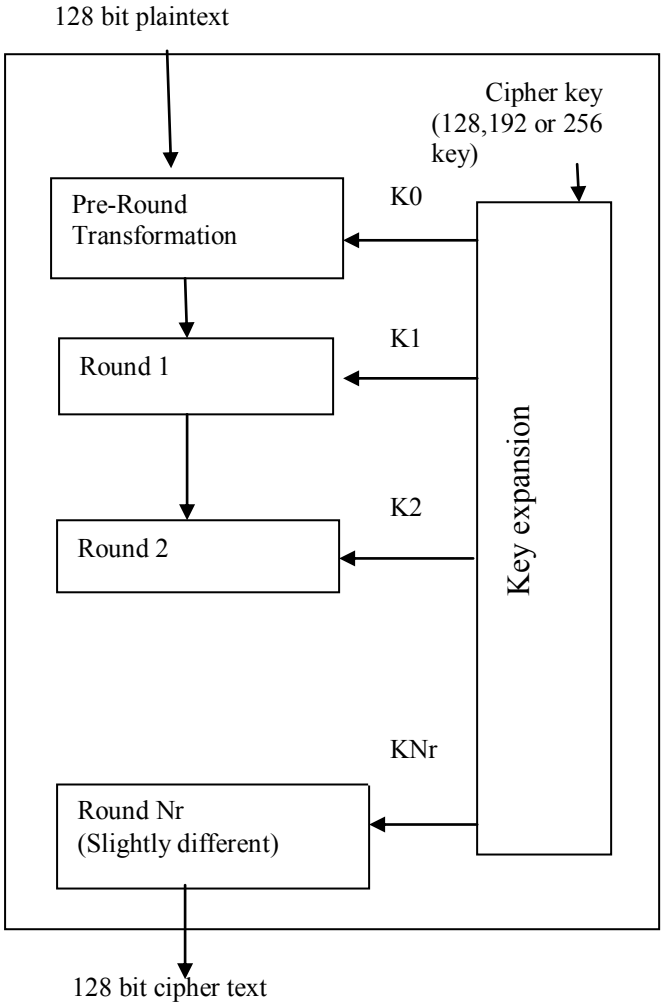
3DES

Triple DES applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. In general TDES was introduced to have three keys .Having a key length of 168 bits: three 56-bit DES keys. When it was discovered that a 56-bit key of DES is not enough to protect from attacks, TDES was chosen as a simple way to enlarge the key space without a need to switch to a new algorithm. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys.

Triple DES with two keys



AES: (Advanced Encryption Standard), also known as the Rijndael algorithm, is a symmetric block cipher. AES is a non- feistel cipher. It uses 10, 12 and 14 rounds .The key size for 10 is128 bit, 12 is192 bit, 14 is 256 bits depends on number of rounds. AES is the relation between time and cost. To provide security, AES uses four types of transformation: substitution, permutation, mixing and key adding. AES was introduced to replace the DES. Brute force attack is the only effective attack known against this algorithm.



NUMBER OF ROUNDS (Nr)	KEY SIZE
10	128
12	198
14	256

Relationship between number of rounds and cipher key size.

ISSN: 2278 – 7798

V.COMPARISON OF DES, 3DES AND AES

DES	3DES	AES
64 bit block of plaintext as input and output as 64 bit block of cipher text.	64 bit block of plaintext as input and output as 64 bit block of cipher text	128 bit block of plaintext as input and output as 128 bit block of cipher text
It has16 rounds.	It has 48 rounds.	It has 10, 12 or 14 rounds.
It uses 56 bit cipher key.	It uses 168 bit key.	It uses 128,192 and 256 bit key.
It has round key of 48 bit.	It has round key of 56 bit.	It has round key of 128 bit.

Key length: 128,192,256 bits; 168,112 bits; 56 bits respectively.
Block Size: 128, 192, 256 bits; 64 bits; 64 bits.
Developed: 2007, 1978, and 1977.
Cryptanalysis resistance:

- Strong against differential
- brute force attacker could be analyzed
- weak substitution
- interpolation and square attacks
- vulnerable to differential

Possible keys: 2128, 2192; 2256, 2112; 2168,256.
Time required checking all possible keys at 50 billion keys per second: For 128-bit key 5×1021; For 112-bit key 800 days; For 56-bit key 400 days.

VIII.CONCLUSION

In this paper a new comparative study between DES, 3DES and AES were presented into various factor, which are key length, cipher type, block size, developed, cryptanalysis resistance, security, and possibility key. The time required to check all possible key at 50 billion second are proved that the AES is better than DES and 3DES.

IX.ACKNOWLEDGMENT

Thanks in advance for those who support me in any way; also I want to thank Mrs. PRIYANKA AGRAWAL for the support. She helped in making this project successful.

.

x.REFERENCES

[1] A.A.Zaidan, B.B.Zaidan, Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", World Academy of Science Engineering and Technology (WASET), Vol.54, ISSN: 2070-3724, P.P 468-479.

[2] A.A.Zaidan, A.W. Naji, Shihab A. Hameed, Fazidah Othman and B.B. Zaidan, "Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File ", International Conference on IACSIT Spring Conference (IACSIT-SC09), Advanced Management Science (AMS).

Rimpi Debnath, BE 8th SEM (CSE), GDRCET Bhilai.

Priyanka Agrawal,Asst.Prof.CSE, GDRCET Bhilai.

Geetanjali Vaishnav, BE 8thSEM (CSE), GDRCET Bhilai.